



Data-Security / Data-Protection

Datenschutz (Data-Protection) / Datensicherheit



Schutz von sensiblen Daten vor...

- anderen Personen
- Verlust von Datenträgern



Datenschutz bei Datenaustausch



Daten können bei Uebermittlung...

- Mitgelesen werden (Kopien)
- Verfälscht werden

Authentifikation

The screenshot shows a PGP key management interface for a contact named Walter Rothlin. The window title is "Walter Rothlin <Walter@Rothlin.com>". At the top, there are buttons for "Add Email Address", "Request Certificate", and "Change Passphrase". Below this is a profile picture of a man and his name "Walter Rothlin" with email "Walter@Rothlin.com". A table of key properties follows:

ID	0x3B42DA95	Created	22.06.2005
Type	RSA	Expires	Never
Size	2048/2048	Group	No
Trust	Implicit	Cipher	AES-256
Validity	Valid	Hash	SHA-2 256
Enabled	Yes	Compression	ZLIB
Keyserver	ldap://keyserver.pgp.com		

Below the table is a "Fingerprint" section with a "Copy" button. It shows a fingerprint icon and two tabs: "Hexadecimal" and "Biometric". The "Hexadecimal" tab is active, displaying the fingerprint:

```
90B7 01B6 0A9C 38C5 1BCC  
80DE AE74 2C78 3B42 DA95
```

At the bottom, there are sections for "Subkeys" and "Revokers". The "Subkeys" section has buttons for "Revoke", "Remove", and "Add", and a table with one entry:

Valid from	Expires	Size	ID
22.06.2005	Never	2048	0x0D6D7425

The "Revokers" section also has "Update", "Remove", and "Add" buttons.

Ist Absender / Empfänger wirklich die Person die ich meine?

- Wie erkenne ich jemanden am Telefon?
- Wie bin ich sicher, dass eine e-mail mit Absender Walter@Rothlin.com wirklich ER ist?

Authentifikation

Rothlin Walter (KETT 2)

Von: Chase Bank [pw-conf@chase.com]

Gesendet: Montag, 20. März 2006 07:54

An: Rothlin Walter (KETT 2)

Betreff: [SPAM] Security Enhancement



Chase Bank is constantly working to ensure security by regularly screening the accounts in our system. We recently reviewed your account, and we need more information to help us provide you with secure service. Until we can collect this information, your access to sensitive account features will be limited. We would like to restore your access as soon as possible, and we apologize for the inconvenience.


Why is my account access limited?

Your account access has been limited for the following reason(s):

- March 19, 2006: We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive **Chase Bank** account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

(Your case ID for this reason is CHSE04-410-320-3334.)

Verschlüsselung (symmetrisch)



Canaanite	Modern
𐤀	A
𐤁	B
𐤂	C
𐤃	D
𐤄	E
𐤅	F
𐤆	G
𐤇	H
𐤈	I
𐤉	J
𐤊	K
𐤋	L
𐤌	M
𐤍	N
𐤎	O
𐤏	P
𐤐	Q
𐤑	R
𐤒	S
𐤓	T

Sender und Empfänger vereinbaren, wie verschlüsselt wird.

Schlüsselaustausch ist das Sicherheitsproblem

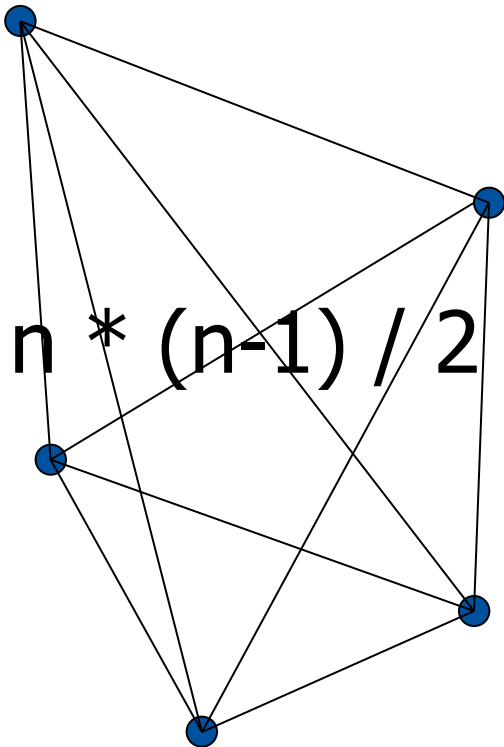
Online-Tool für symmetrischer Verschlüsselung

<https://8gwifi.org/CipherFunctions.jsp>

Verschlüsselung (symmetrisch)

Es benötigt pro Verbindung einen Schlüssel!

Schlüsselverwaltung + Schlüsselaustausch
problematisch



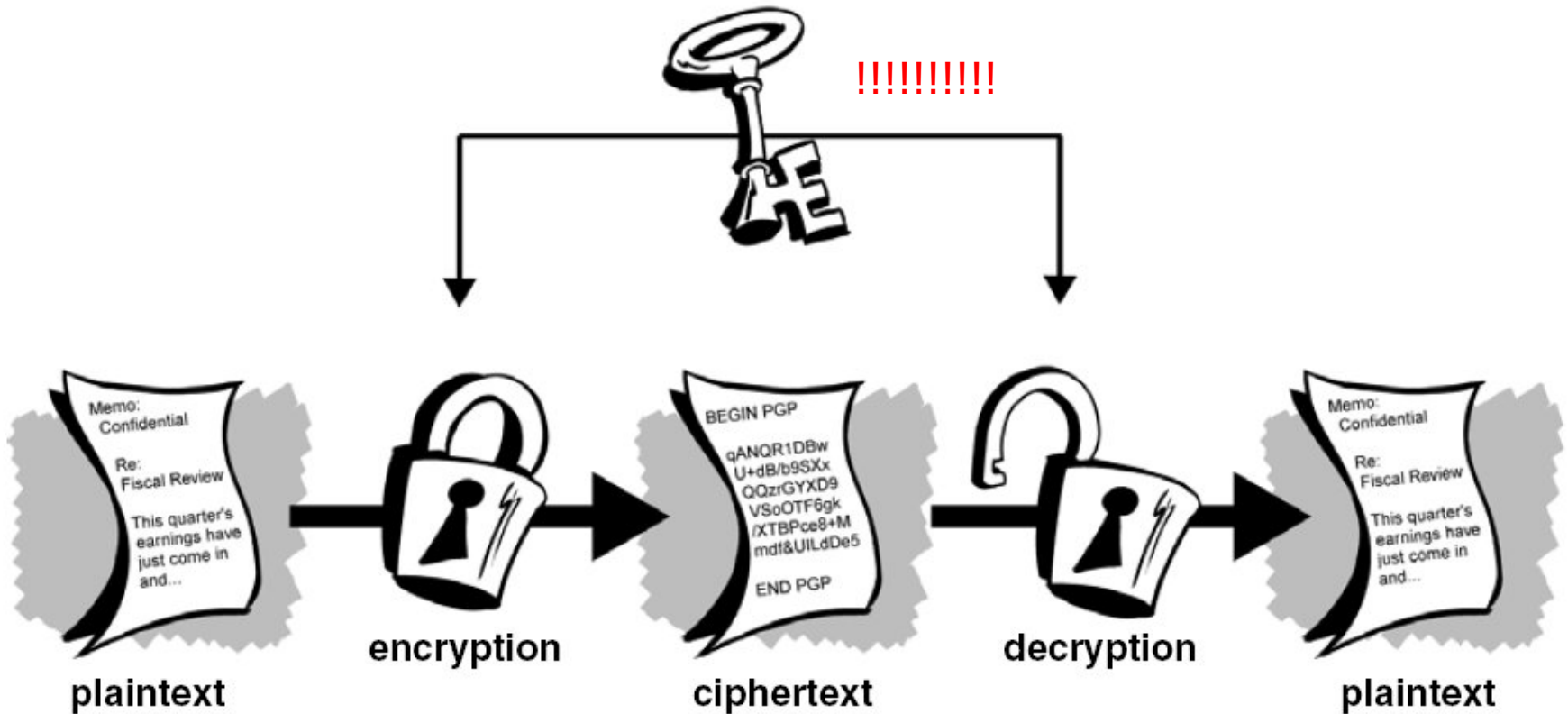
Binominalkoeffizient (Gelesen: n tief k oder k aus n)

→ Taschenrechner nCr

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} =$$

$$= \frac{\overbrace{n * (n-1) * (n-2) * (n-3) * \dots}^{k \text{ Faktoren}}}{k!}$$

Verschlüsselung (symmetrisch)



Verschlüsselung (asymmetrisch)

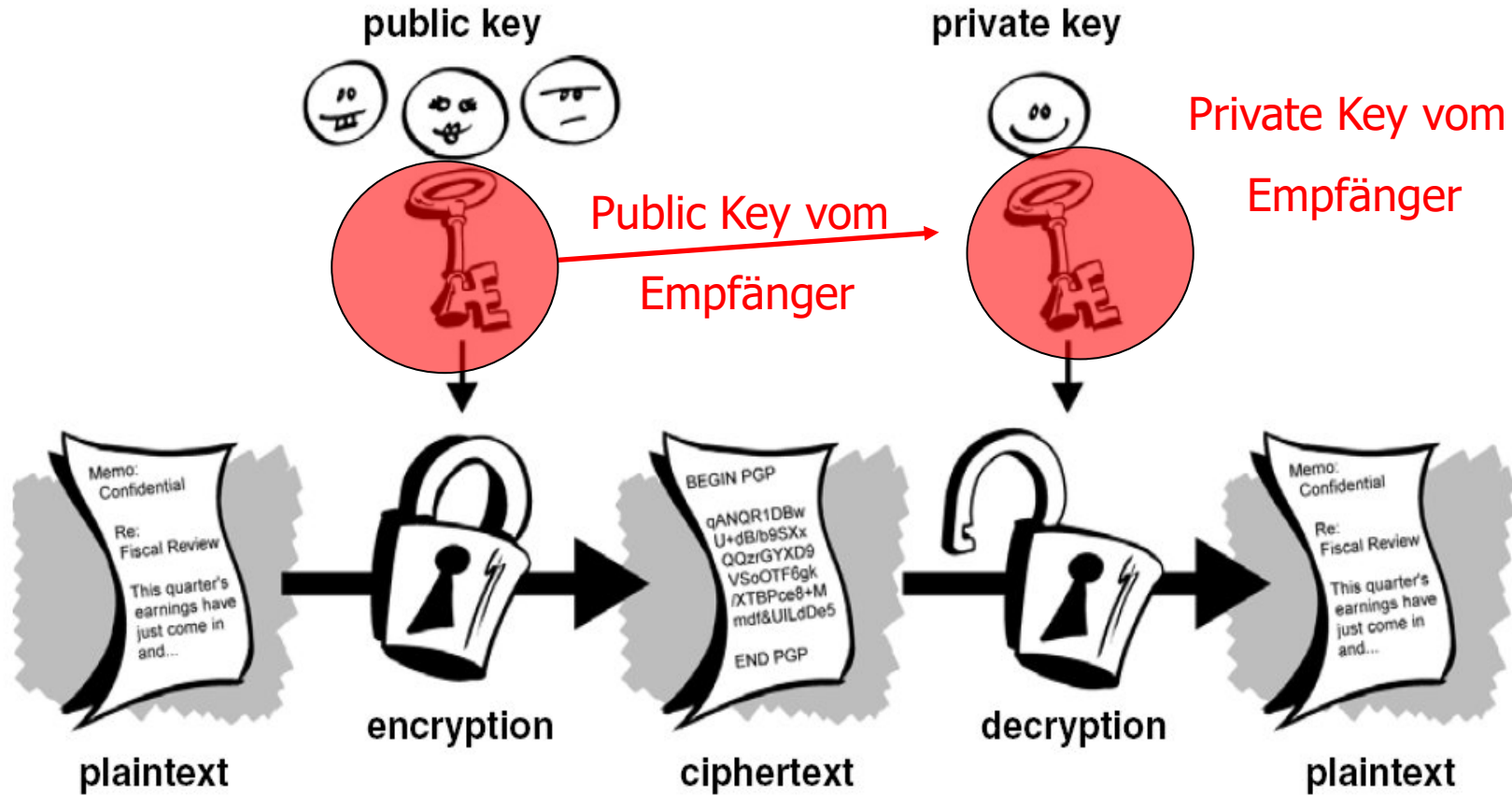
Jeder Kommunikationspartner hat einen
Public- und einen **Private**-Key

Verschlüsselt wird mit dem
Public-Key des **Empfängers**

Entschlüsselt wird mit dem
Private-Key des **Empfängers**

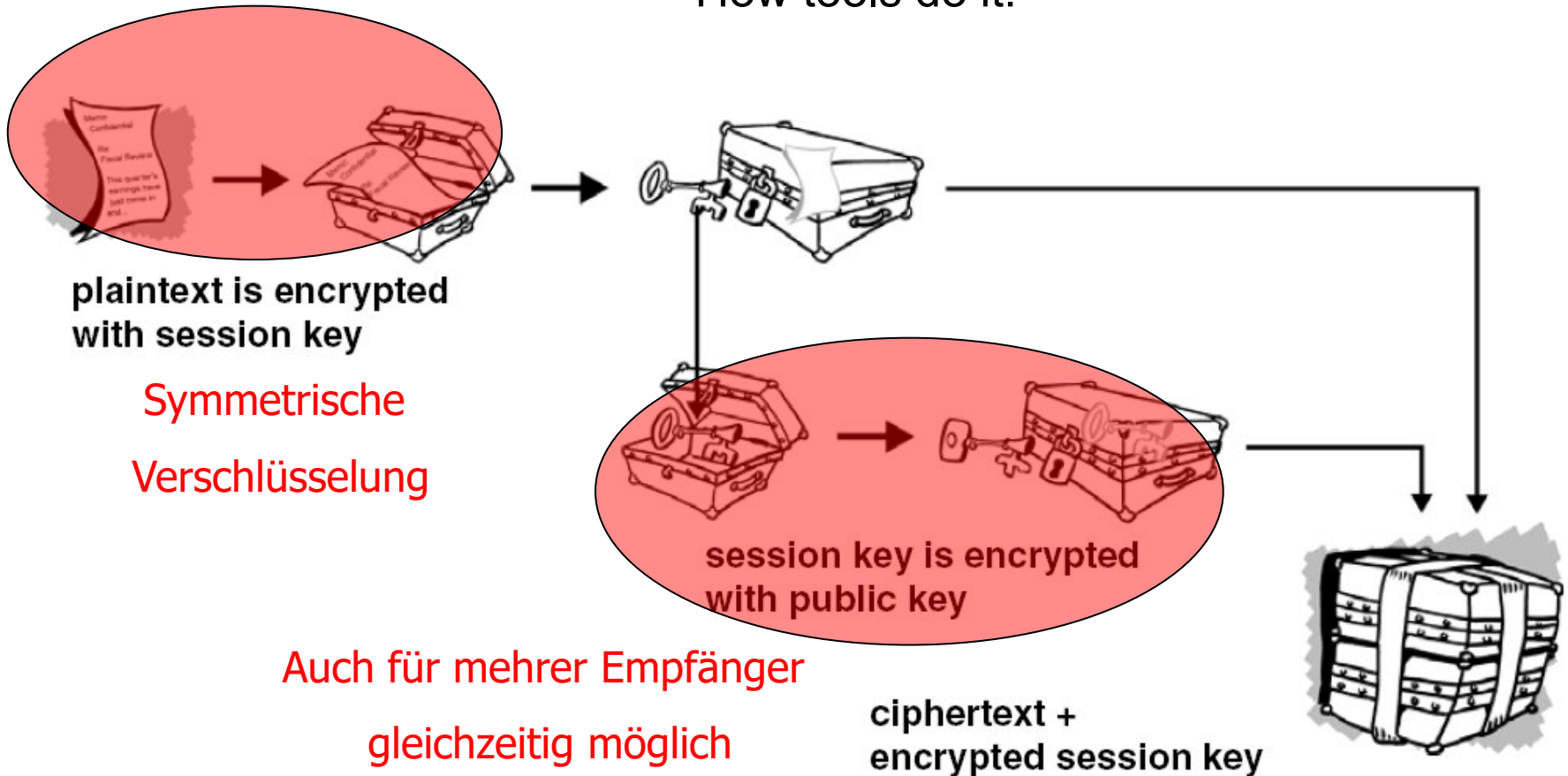
Verschlüsselung (asymmetrisch)

Public – Private Key Encryption (PPK)

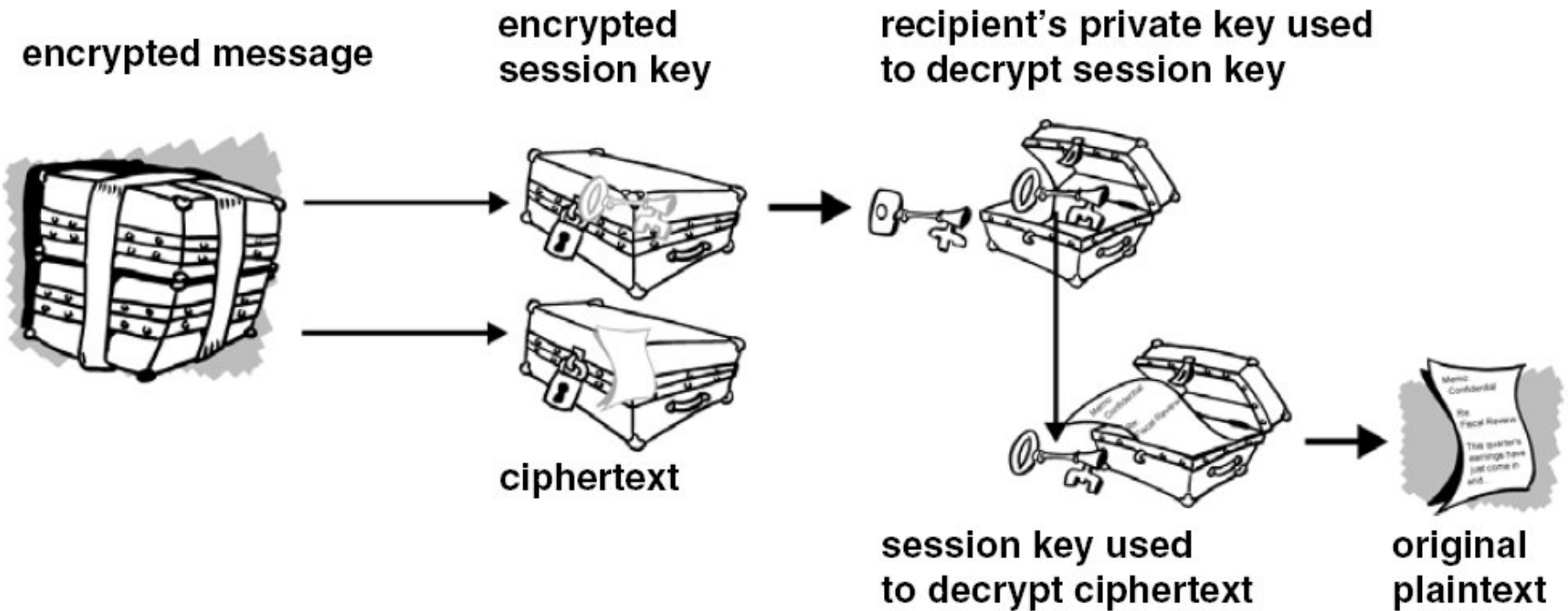


Verschlüsselung (asymmetrisch)

How tools do it!

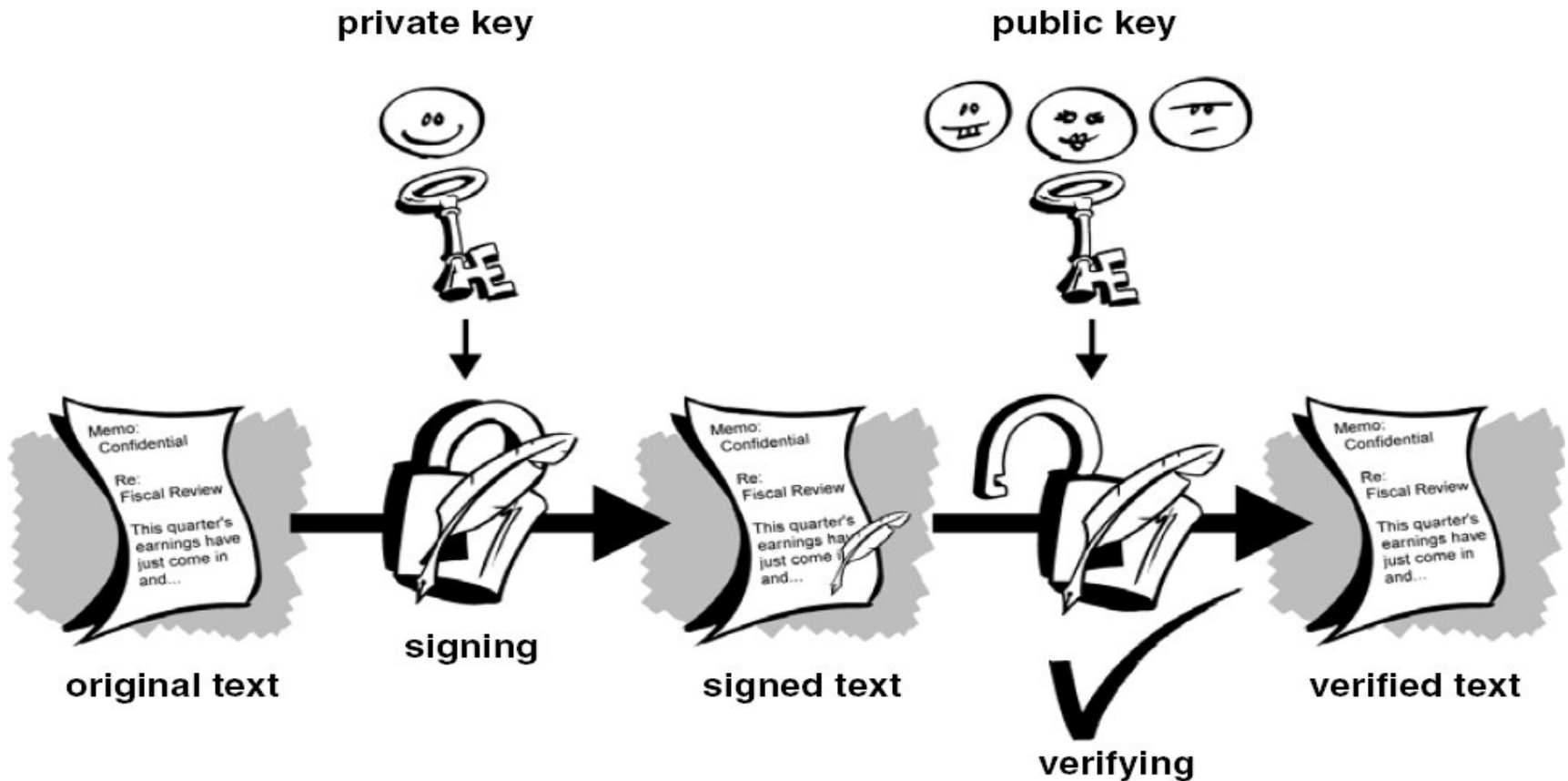


Verschlüsselung (asymmetrisch) How tools do it!

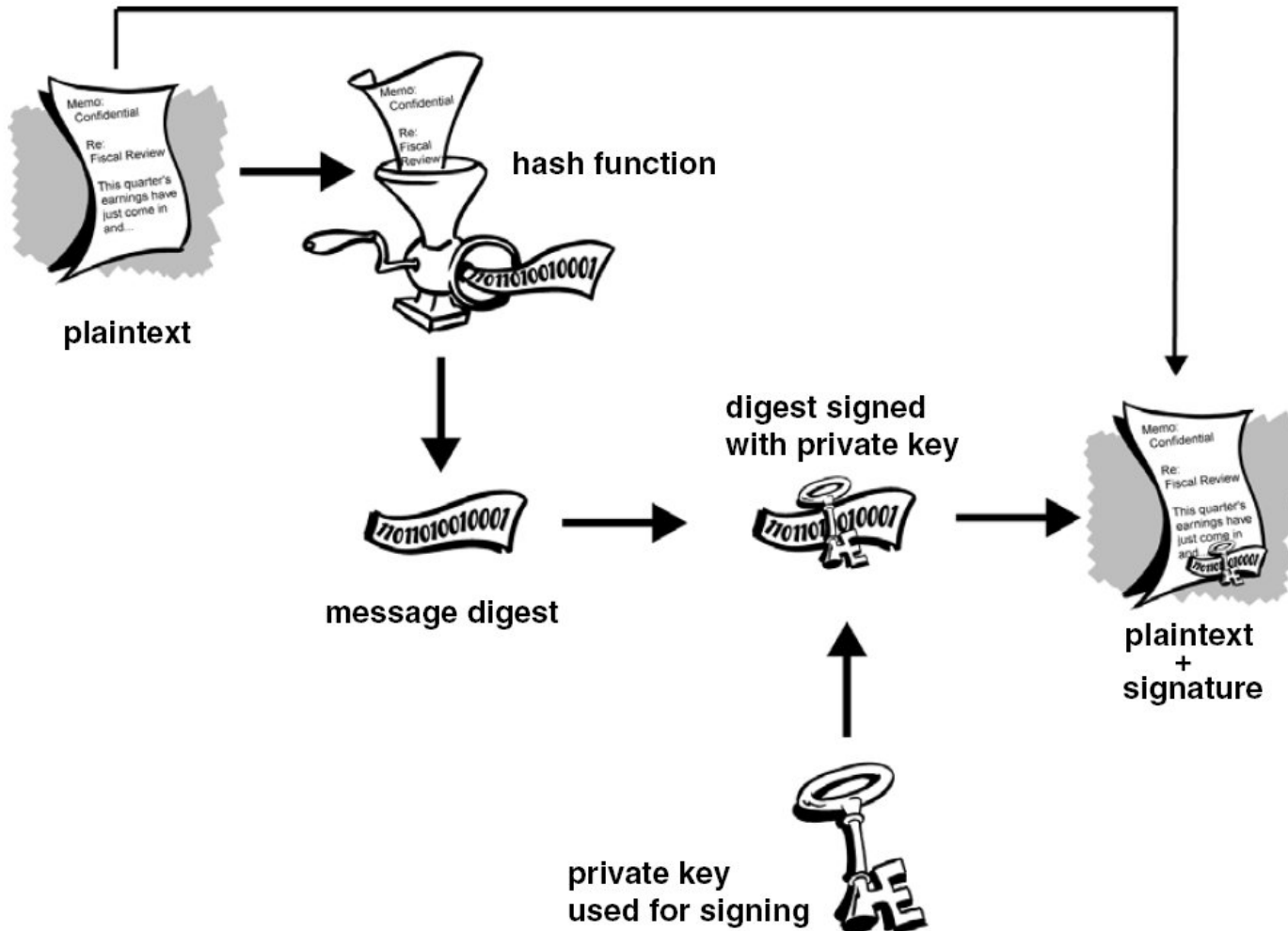


Visieren (Signing)

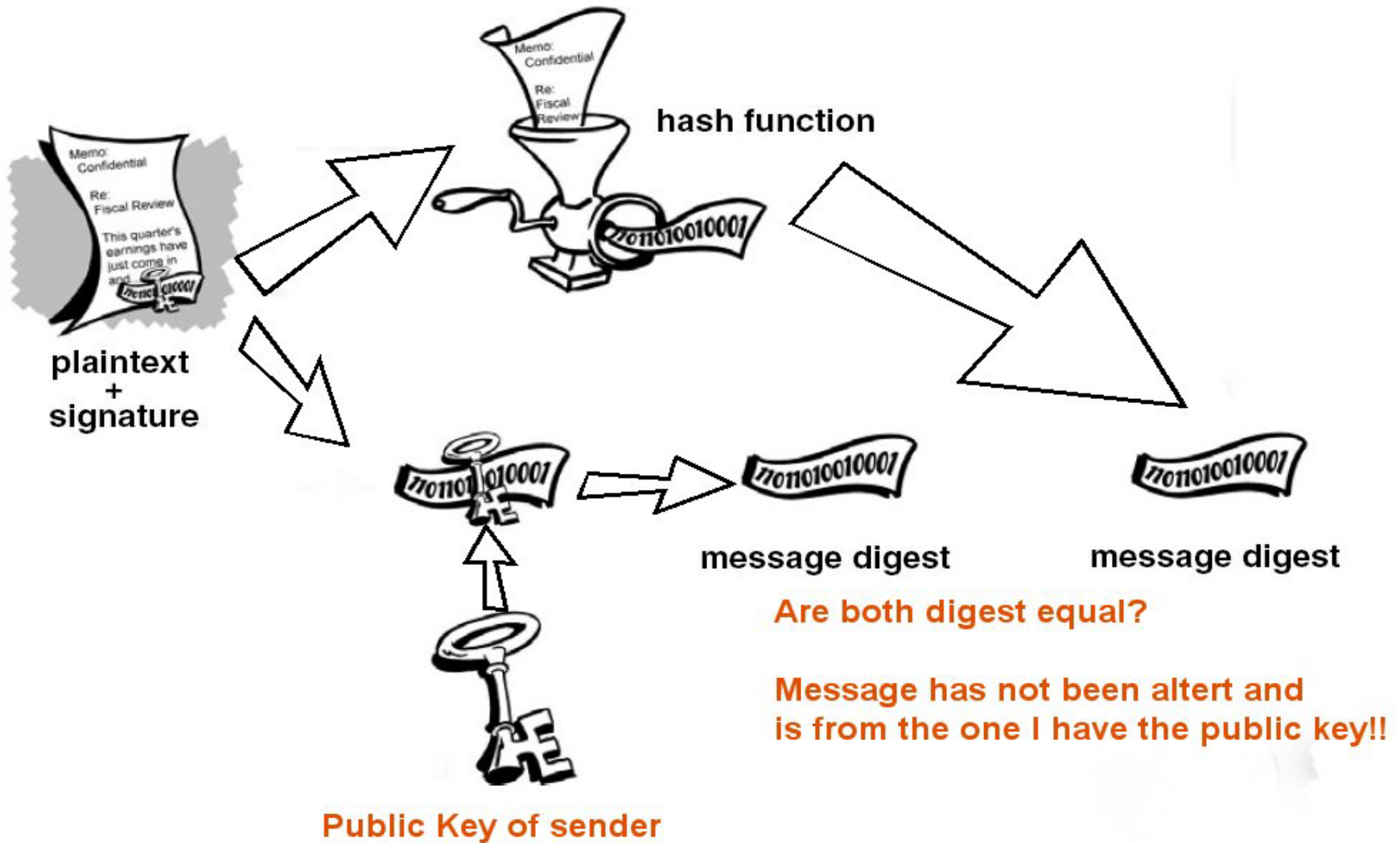
Private Key kann auch für Verschlüsselung verwendet werden!



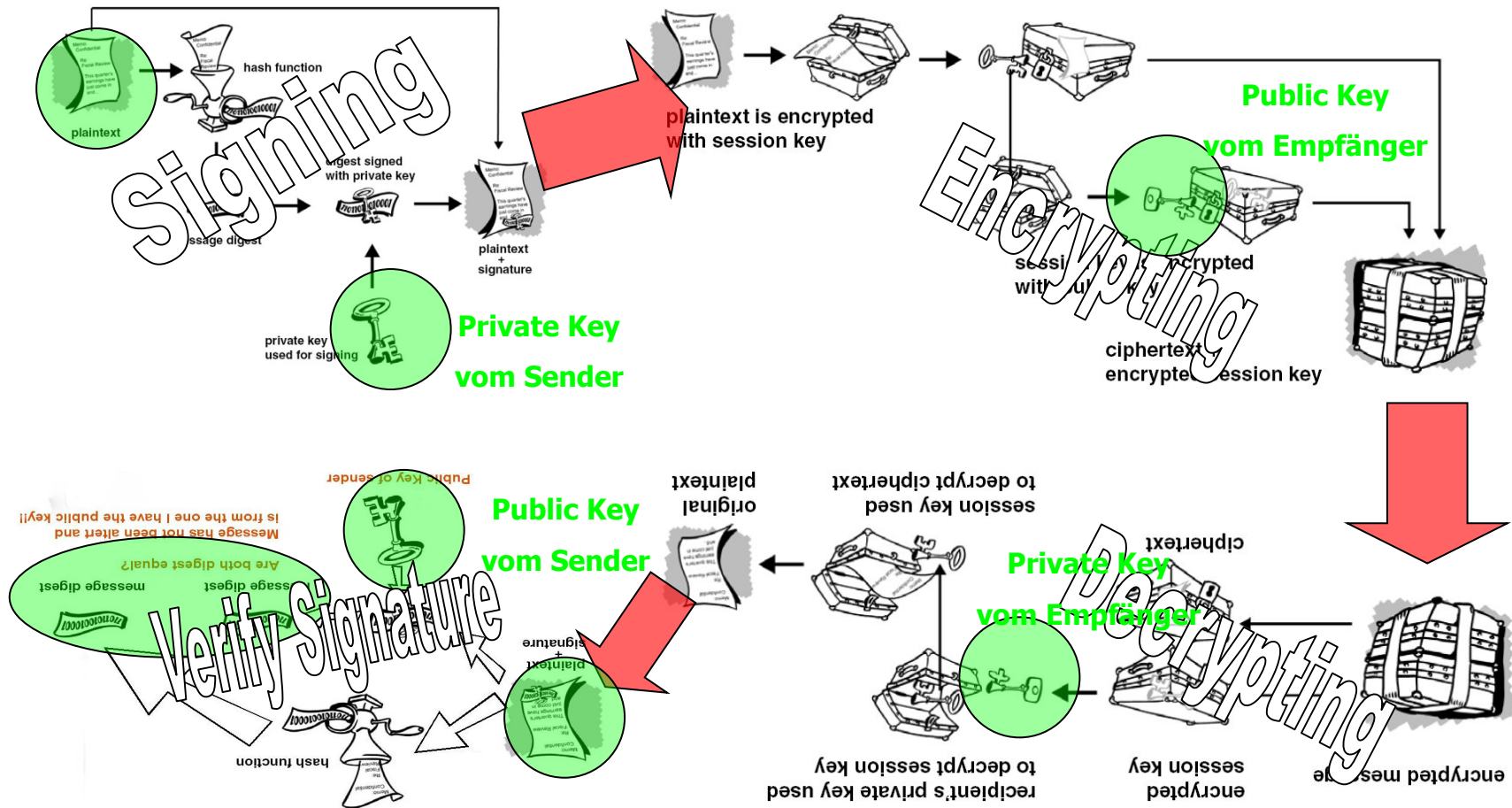
Visieren (Signing) How tools do it!



Visieren (Verifizieren)



Visieren und Verschlüsseln



Anforderungen an Sicherheit und deren Erfüllung

Vertraulichkeit (confidentiality)

- Bsp. Aktien-Kauf: *Finanzamt soll aber nicht erfahren, was ich mit Aktien mache*
- Kommunikationsflüsse beschränken/absichern

Integrität

- *keine Fälschung „Verkauforder“ zu „Kauforder“*
- Unautorisierte Manipulation verhindern

Authentizität

- *Bank und ich wollen gegenseitig wissen, wer was macht – wo landet denn mein Geld?*
- Eindeutige Identifikation der Subjekte

Verbindlichkeit (non-repudiation)

Verfügbarkeit

Anonymität

Sicherheitsmechanismen & -verfahren: Realisierung

Vertraulichkeit

- Kryptographische Verfahren: symmetrische, asymmetrische, z.B. DES, (AES), IDEA, Twofish, RC4, A3, A5, A8, RSA, El-Gamal
- Sicherheitsklassifikation (labeling) & Beschränkungen, z.B. Bell LaPadula: no-read-up, no-write-down

Authentizität

- Wissensbasiert: Passwortverfahren, Challenge-Response, Message Authentication Codes (MAC), Passworte z.B. S/KEY, PINs; Zertifikate z.B. X.509, MAC-Verfahren z.B. MD5, HMAC-MD5
- Besitzbasiert: Chipkarte, Smartkarte z.B. SIM-Karte in GSM
- Biometrie: Fingerabdruck, Iris-, Retina-Scanner etc.

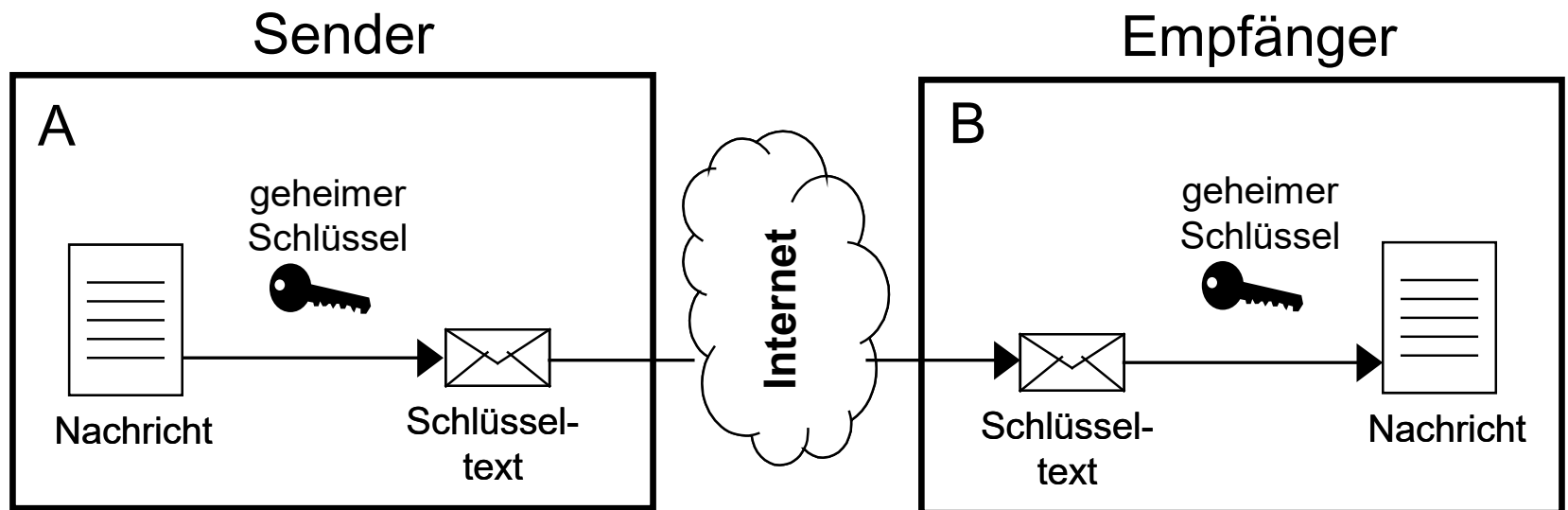
Datenintegrität

- Hashfunktionen, Prüfsummen: z.B. MD5, SHA-1
- Zugriffskontrolllisten ACL, Capabilities, Zugriffstickets

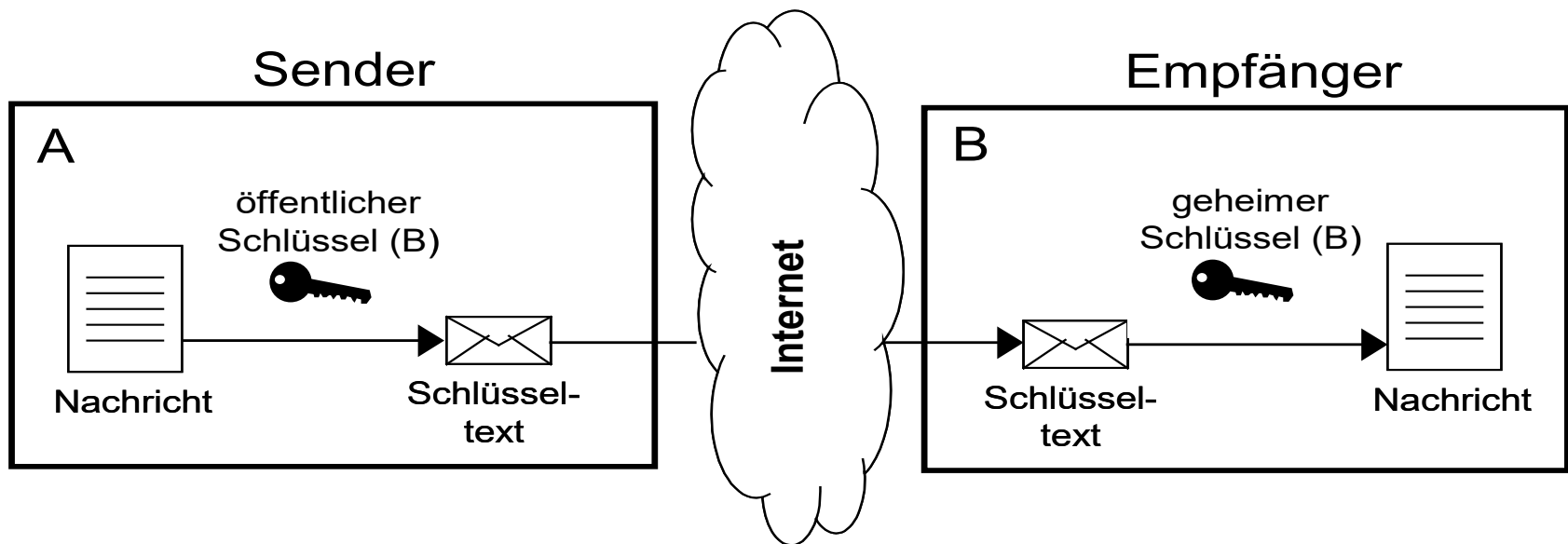
Verbindlichkeit: digitale Signaturen: z.B. DSA, RSA

Verfügbarkeit: Netzüberwachung, Filterungen

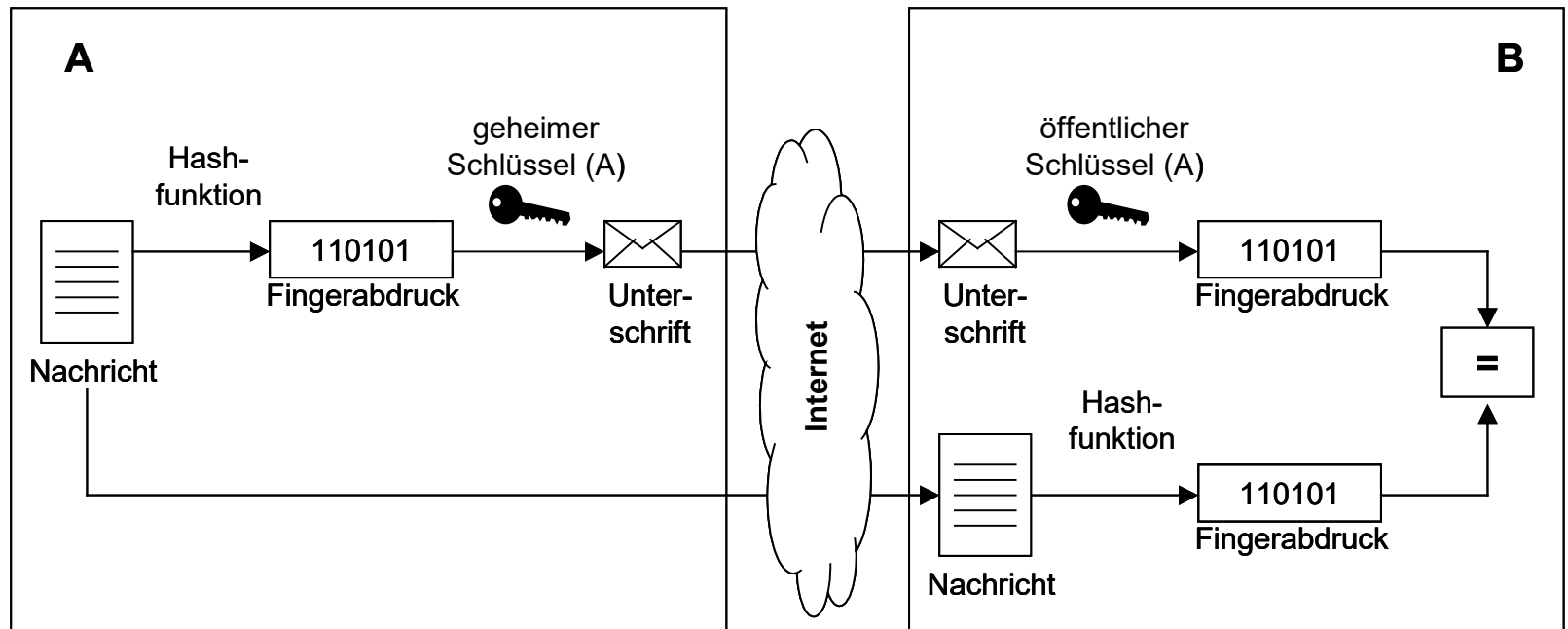
Symmetrische Verschlüsselung



Asymmetrische Verschlüsselung



Digitale Signatur

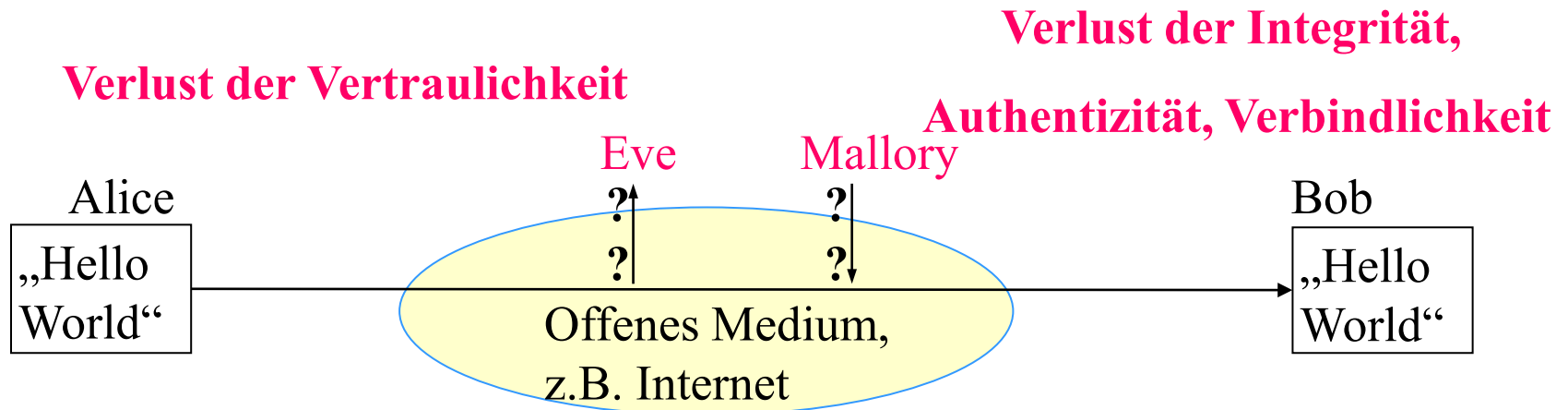


Ausgangslage für Kryptosysteme

Alice will Bob eine Nachricht schicken,

Eve soll den Inhalt der Nachricht nicht erfahren (Vertraulichkeit)

Mallory soll keine Chance haben, den Inhalt der Nachricht unerkannt zu verfälschen oder falsche Nachrichten abzuschicken (Integrität und Authentifizierung).



Ablauf einer verschlüsselten Kommunikation

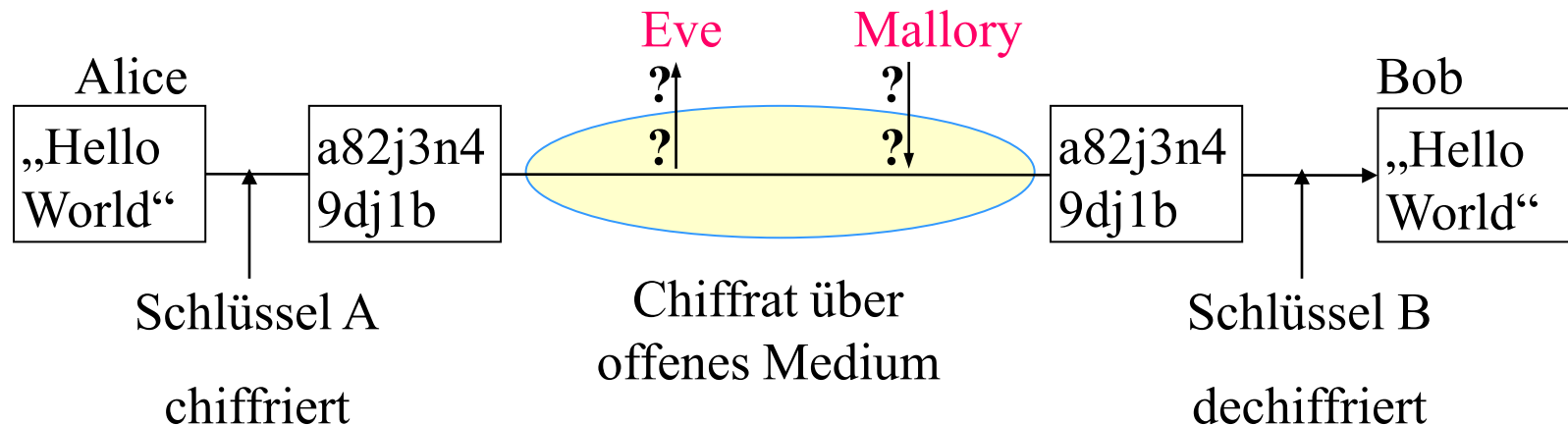
Alice **verschlüsselt** / **chiffriert** Nachricht („**Klartext**“) mit Hilfe ihres **Schlüssels** und einer **Verschlüsselungs-** oder auch **Chiffrierfunktion**.

Alice schickt **Chifftrat** / **Kryptogramm** an Bob

Bob nutzt eigenen Schlüssel und eine **Entschlüsselungs-** oder **Dechiffrierfunktion** zur Umwandlung in Klartext

Idealfall

- Eve kann mit Chifftrat die ursprüngliche Nachricht nicht erlangen
- Eine Änderung durch Mallory fällt Bob sofort auf



IDEA (International Data Encryption Algorithm)

symmetrische Blockchiffre, Blocklänge 64 Bit, feste Schlüssellänge 128 Bit.

Ver- und Entschlüsselung:

- gleicher Algorithmus
- Dechiffrierschlüssel leicht aus Chiffrierschlüssel zu bestimmen.

Hilfsmittel

- Erzeuge 52 Unterschlüssel, indem man den 128 Bit langen Schlüssel in acht 16 Bit lange Unterschlüssel zerteilt.
- Die nächsten 8 Unterschlüssel erhält man, indem man die Bits des Schlüssels um 25 Positionen nach links rotiert und dann den Schlüssel in acht Segmente zerteilt und so weiter.

Asymmetrische Kryptosysteme – allgemeiner Ablauf

Kommunikationspartner Alice & Bob erzeugen sich jeweils ein Schlüsselpaar $(ek_{\text{alice}}, dk_{\text{alice}})$ bzw. $(ek_{\text{bob}}, dk_{\text{bob}})$

- ek Schlüssel: öffentlich (in ein Verzeichnis)
- dk Schlüssel: geheim

Alice **verschlüsselt** M mit dem öffentlichen Schlüssel ek_{bob} von Bob: $\mathbf{C = enc(M, ek_{bob})}$

Versenden der Nachricht C von Alice zu Bob

Bob **entschlüsselt** C mit seinem privaten Schlüssel dk_{bob} : $\mathbf{M = dec(C, dk_{bob}) = dec(enc(M, ek_{bob}); dk_{bob})}$

Anwendungen – sicherer Transfer: SSL

SSL (Secure Socket Layer): kryptographisch gesicherte Übermittlung von Informationen im Internet

Wichtige Aspekte

- 40-bit SSL unsicher => 128-bit zu bevorzugen
- **Hybrides Verfahren**
 - Zuerst RSA
 - Dann symmetrisches Verfahren: höheren Geschwindigkeit dieser Kryptosysteme. (Sonst zusätzliche Transaktionskosten).
- RSA: Schlüssel mehrfach, daher höhere Sicherheit. Symmetrisches Verfahren: nur für den Schutz einer Übertragung.

Anwendung: Erzeugung und Nutzung Digitale Signatur

Eigenschaften handschriftlicher Unterschriften auf digitale Welt übertragen

Probleme: u.a. leichtes Ausschneiden, Kopieren, Verfälschen digitaler Muster

- **Signaturerstellung** meist mit **asymmetrischen** Verfahren
- Idee: Alice signiert mit dem privaten, geheimen Schlüssel ek_{alice} : $\text{sig} = \text{dec}(M, dk_{\text{alice}})$
- Verifikation der Signatur mit zugeordnetem öffentlichen Schlüssel: $M = \text{enc}(\text{sig}; ek_{\text{alice}})$
- Gewährleistung von Authentizität und Vertraulichkeit
 1. Verschlüssele mit öffentlichen Schlüssel des Empfängers
 2. Verschlüssele mit geheimen Schlüssel des Senders (s.o.)

Zertifikate

Problem: Authentizität des öffentlichen Schlüssels ek_{alice} zusichern!

Benötigt: Vertrauenswürdige Instanz (CA) (Trust Center, Certification Authority): signiert ek_{alice} mit dk_{ca}

Problem: Authentizität von ek_{alice} ! Das eigentliche Problem wurde delegiert...

Infrastruktur für Zertifikate notwendig: PKI Public-Key Infrastructure

Beispiel für ein Zertifikat: X.509 (Auszug)

- Versionsnummer beschreibt verwendetes Zertifikatformat
- Seriennummer eindeutiger Identifikator
- Signatur verwendete Algorithmen und Parameter
- Zertifikataussteller Name der ausstellenden Instanz
- Gültigkeitsdauer Angabe eines Zeitintervalls
- Benutzername eindeutiger Name des Benutzers

Public Key:

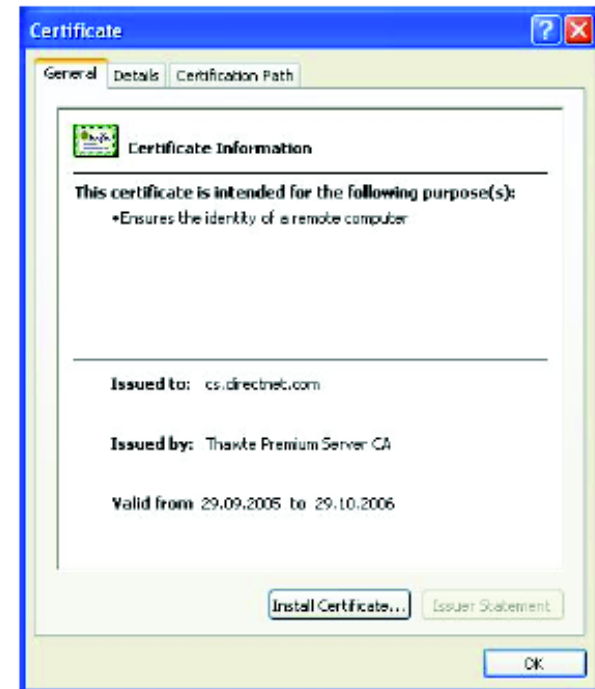
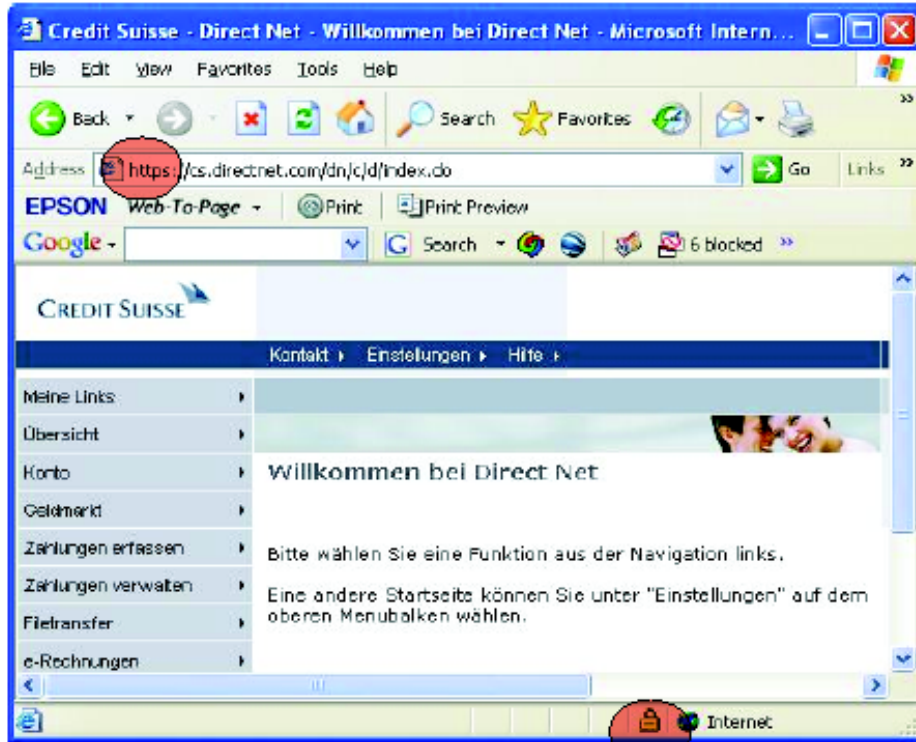
- URL für Download auf Visitenkarte
- Attached an jedes e-mail

Private Key:

- Auf Computer Hard-Disk (Backup im Safe)
- Smartcard
- Cryptokey
- Mit einem Passwort geschützt

Public Key Zertifikate

- Bindet ein Public Key mit einer Identität zusammen
- Name, Geburtsdatum,... ist im Certificate
- Certificates werden von der Ausgabestelle elektronisch visiert
- Ausgabestelle: Certificate Authority (CA)
- SSL: Secure Socket Layer (https)



- Strichlisten
- SecureID Card
- PKI: Public Key Infrastructure
- GPG (GNU Privacy Guard)
 - Open Source PGP
 - Download for Windows
<http://www.gpg4win.org/index.html>

Viren, Würmer, Trojaner

- Alle drei können Daten zerstören oder Informationen weitergeben
- Viren hängen sich an eine Datei und werden durch kopieren dieser Datei verbreitet.
- Würmer nutzen einen Dienst vom Computer (e-mail, Netzwerkfunktionen) um sich selbständig auf andere Systeme zu kopieren.
- Trojaner (Trojanisches Pferd) gibt etwas anderes vor als es macht

Viren, Würmer, Trojaner

- Anti-Virus Software aktuell halten
(Serum nachladen)
- Vorsicht beim Download und kopieren
- Misstrauue jedem e-mail
- Windows um mehrfaches mehr gefährdet als
LINUX, UNIX oder MAC

Firewall und Proxy-Server

- Firewall: Durch diese Gasse muss er kommen
 - Regeln was erlaubt ist müssen definiert sein
 - Genaues loggen was passiert
-
- Proxi: Stellvertreter
 - Regeln was erlaubt und was verboten ist
 - Genaues loggen aller Requests
 - Cashing möglich

Verschlüsselt oder Unverschlüsselt

Lieber Chef! Mein Assistent, Herr Meyer, ist immer dabei, seine Zeit mit Schwätzchen mit seinen Kollegen zu verplempern. Nie schafft er sein Arbeitspensum; und sehr oft bleibt er länger in der Mittagspause. Mein Assistent ist jemand ohne Computerkenntnisse. Er ist einer der Mitarbeiter, auf die man gern verzichtet. Ich denke, dass es Zeit wird für ihn, zu gehen. Die Firma kann davon nur profitieren

Aber: am Ende steht immer der Mensch

- Zugriff für Unberechtigte vermeiden!
Aufräumen, Abschliessen, Vernichten,
- Sich an Regeln halten und Weisungen befolgen!
auch wenn immer alles problemlos ging
- Andere sensibilisieren es auch zu machen

➔ Wissen ist vorhanden. Am Machen scheitert es!

Generiertes Schlüsselpaar

<https://8gwifi.org/pgpkeyfunction.jsp>

PGP Key Generate

Identity

walter@rothlin.com

Passphrase

•••••• BZU_007

Algo ☒ BLOWFISH ☐ TWOFISH ☐ AES_256 ☐ AES_192 ☐ AES_128 ☐ CAST5 ☐ TRIPLE_DES

Key Size ☒ 1024 ☐ 2048 ☐ 4096 (Performance Suffer)

Generate Keypair

Email Key Pair

Generiertes Schlüsselpaar

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: BCPG v1.58

IQH+BGC4rkUBBADeR6i7bfaUScOPQkIUS+3bz5nqxDeGIPpTEosBpz/MxHBI+Opt
TpWL4XJoa8jGrrcxXBQgQG1DFn/iWHRXgVnbf8lZWzmEI/z95KmfiKceRkcGiKh/
61aP9cQc+lrX1BDCdKubi6RmKc1NiwnlogCmrLv/ieCwQzjGZaXZ3aMpgwARAQAB
/gQDAsiVR9zzhdXGYLS2gzwNMS8HIVyS4uVmHcKvNFmQ4Khx5tDx4XcDgW8naXO
gjxQKwg0uRHs1DaLygaX97Ks5myzoPQhVqBW7HuKpHq3cEMdhJQklISNW9GOK0tX
D7DJPDhNpMCw9hXcqohxrE70znFxYZSBoFVLe0WWdKbe1Vpw/yAz4dnrpCIGMeKb
nP9kNmaNIYUfVJxtfAaExm1CYYKmFDsJ6dcNFGVdjA56DI47gGKQueb5z9Rbv3sT
IITWgIRSw9grQ3jNFLyD/bYGB8x3ibTWbO1T3zKD1rbxrv8UIUnO0cwZcnobm2xc
U5VK7GB37Fgmlz9iDzdfZvXEf51s5D+JrYIPgMO+ynd0QqL0e3Vs/BYN76Wnv0Za
ACfM/O80xadh6oo80XXq7SUwMLOOFbBrDXagT9mF4clSMqVqUcQb0jU18Kdl0koA
alFsxdzB4q52kOG3vIVJUzdXVh9oxETgJcgaJe/N3UYOtBJ3YWx0ZXJAcM90aGxp
bi5jb22lnAQQAQIABgUCYLiuRQAKCRDTie6xLQzYq35hA/9NqPRQMmEM1nVr/V6Q
3Z5pS2l3MHEYH9TsWMbRrn21Yt8dfUy8VNmmgRZ2RdilvA7bIWbPQbXSCaulrjdT
dpBrix5OBkqhLz6XnBNgBzjcu4zPmKnR/yeYjmg2APlzEzmd7jOBVcnWRMUWky/r
dQAB3nwPLM0Gr/hbFy8TEwGLdQ==

=EvKV

-----END PGP PRIVATE KEY BLOCK-----



Generiertes Schlüsselpaar

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: BCPG v1.58

mI0EYLiuRQEEAN5HqLtt9pRJw49CQhRL7dvPmerEN4aU+IMSiwGnP8zEcEj46m1O
nAvhcmhryMautzFcFCBAbUMWf+JYdFeBWdt/yVlbOYSX/P3kqZ+Ipx5GRwalqH/r
Vo/1xBz6WtfUEMJ0q5uLpGYpzU2LCciiAKasu/+J4LBDOMZlpdndoymDABEBAAG0
EndhbHRlckByb3RobGluLmNvbYicBBABAgAGBQJguK5FAAoJENOJ7rEtDNirfmED
/02o9FAyYQzWdWv9XpDdnmlLaXcwcRgf1OxYxtGufbVi3x19TLxU2aaBFnZF2KW8
DtshZs9BtdIJq4iuN1N2kGuLHk4GSqEvPpecE2AHONy7jM+YqdH/J5iOaDYA8jMT
OZ3uM4FVydZExRaTL+t1AAHefA8szQav+FsXLxMTAYt1

=u1K9

-----END PGP PUBLIC KEY BLOCK-----



Meldung verschlüsseln

PGP Encryption & Decryption

<https://8gwifi.org/pgpencdec.jsp>

Encrypt/Decrypt PGP Message

☒ Encrypt message

☐ Decrypt message

Clear Text Message

Bitte überweisen Sie eine Milion an meine Frau!



-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: BCPG v1.58

ml0EYLiurQEEAN5HqLtt9pRJw49CQhRL7dvPmerEN4aU

+IMSiwGnP8zEcEj46m1O

nAvhcmhryMautzFcFCBAbumWf+JYdFeBWdt/yVlbOYSX

PGP Public Key

PGP MESSAGE

-----BEGIN PGP MESSAGE-----

Version: BCPG v1.58

hlwD04nusS0M2KsBA/oC8sBpxAA8QLa7PyIT4BhjPuNgySNhMo/mJ2aT7Ulcylb
LruMWjnOs/mZ3IAAf3GlbX0WRiJr8WJ4G/W9YZaWzQYyYifOphd2wXG1wczIEUYo
FuLXMxgg9niVn1bKJZN1o/6eDNCU8B+/sha/bfWpNiSeuUGnVnEQVrykVU8zINJ9
AbKCioWJi4iTBmZjjnSjwTgoRgmtzvtaEzHD3TCvPW9R//3LBExAtDUqYfgwNqXK
y06dNLLWqFY49/+kBEvdMzfk7lj7oHSaeQf+T+UVIdvqVzj175Y/Cr57PIBQUqeE
5eGQ/xHquAzTpJBqDym1SufcOTIjwe+1ZO5XhWM=
=9niJ

-----END PGP MESSAGE-----

Verschlüsselte Meldung

Bitte überweisen Sie eine Million an meine Frau!

-----BEGIN PGP MESSAGE-----

Version: BCPG v1.58

hlwD04nusS0M2KsBA/oC8sBpxAA8QLa7PyIT4BhjPuNgySNhMo/mJ2aT7Ulcylb
LruMWjnOs/mZ3IAAf3GlbX0WRiJr8WJ4G/W9YZaWzQYuYifOphd2wXG1wczIEUYo
FuLXMxgg9niVn1bKJZN1o/6eDNCU8B+/sha/bfWpNiSeuUGnVnEQVrykVU8zINJ9
AbKCioWJi4iTBMzjjnSjwTgoRgmtzvtaEzHD3TCvPW9R//3LBExAtDUqYfgwNqXK
y06dNLLWqFY49/+kBEvdMzfk7lj7oHSaeQf+T+UVldvqVzj175Y/Cr57PIBQUqeE
5eGQ/xHquAzTpJBqDym1SufcOTIjwe+1ZOsXhWM=
=9niJ

-----END PGP MESSAGE-----

Meldung entschlüsseln

PGP Encryption & Decryption

<https://8gwifi.org/pgpencdec.jsp>

Encrypt/Decrypt PGP Message

- ☐ Encrypt message
☒ Decrypt message

PGP Message

-----BEGIN PGP MESSAGE-----

Version: BCPG v1.58

hlwD04nusS0M2KsBA/oC8sBpxAA8QLa7PyIT4BhjPuNgySNhMo/mJ2aT7UlcDylb
LruMWjnOs/mZ3IAAf3GlbX0WRiJr8WJ4G/W9YZaWzQYuYifOphd2wXG1wczIEUYo
FuLXMxgg9niVn1bKJZN1o/6eDNCU8B+/sha/bfWpNiSeuUGnVnEQVrykVU8zINJ9
AbKCiOwJi4ITBMzjjnSjwTgoRgmtzvtaEzHD3TCvPW9R//3LbExAtDUqYfgwNqXK



PGP Private Key

-----BEGIN PGP PRIVATE KEY BLOCK-----

Version: BCPG v1.58

IQH+BGC4rkUBBAdE6i7bfaUScOPQklUS+3bz5nqxDeGIPpTEosBpz/MxHBI+Opt
TpwL4XJoa8jGrrcxXBQgQG1DFn/iWHRXgVnbf8lZWzmEI/z95KmfiKceRkcGiKh/
61aP9cQc+lrX1BDcDkUbi68mKc1Niwnloocmrlv/ieCwOziGZaXZ3aMn0wARAQAB



Passphrase

••••••

BZU_007

Decrypt PGP Message

Bitte ?berweisen Sie eine Milion an meine Frau!
message integrity check passed